This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/054063-2025

Tender

# Data Centre Infrastructure Service

NETWORK RAIL INFRASTRUCTURE LIMITED

UK4: Tender notice - Procurement Act 2023 - view information about notice types
Notice identifier: 2025/S 000-054063
Procurement identifier (OCID): ocds-h6vhtk-052ae4
Published 4 September 2025, 4:28pm

This is an old version of this notice. View the latest version.

## Scope

### Reference

Bravo Project Number 43571

### Description

This project is for a single partner to provide data centre infrastructure services (DCIS).

The scope of the contract covers services needed to support NRIL's data centre infrastructure hosted within data centers, LAN/Edge compute rooms and Cloud Platforms. It includes networks (LAN and WAN), platforms, mainframe, servers, specified applications including tools and services required to effectively operate the infrastructure.

### Total value (estimated)

- £185,300,000 excluding VAT

- £222,360,000 including VAT

Above the relevant threshold

## Contract dates (estimated)

- 9 December 2026 to 10 October 2033

- 6 years, 10 months, 2 days

## Options

The right to additional purchases while the contract is valid.

Optional Capex Projects and Great British Rail transition services.

## Main procurement category

Services

## CPV classifications

- 72222300 - Information technology services

- 48800000 - Information systems and servers

- 72267100 - Maintenance of information technology software

- 72223000 - Information technology requirements review services

## Contract locations

- UK - United Kingdom

---

# Participation

## This procurement is reserved for

Supported employment providers

## Legal and financial capacity conditions of participation

Please refer to PSQ documentation and Appendices in the Bravo portal.

## Technical ability conditions of participation

Please refer to PSQ documentation and Appendices in the Bravo portal.

---

# Submission

## Enquiry deadline

26 September 2025, 1:00pm

## Submission type

Requests to participate

## Deadline for requests to participate

10 October 2025, 4:00pm

## Submission address and any special instructions

https://networkrail.bravosolution.co.uk/

## Tenders may be submitted electronically

Yes

## Languages that may be used for submission

English

## Suppliers to be invited to tender

2 to 5 suppliers

Selection criteria:

Conditions of participation

## Award decision date (estimated)

12 October 2026

## Recurring procurement

Publication date of next tender notice (estimated): 12 October 2026

## Award criteria

| Name | Description | Type | Weighting |
|------|-------------|------|-----------|
| Technical | The below Award Criteria shall be weighted against 65% overall Technical Weighting. Transition Delivery - 13% Service Operations & Governance - 40% Transformation & Optimisation - 15% Innovation - 5% Project Delivery - 10% Social Value - 17% | Quality | 65% |
| Commercial | The below Award Criteria shall be weighted against 35% overall Commercial Weighting. Base charges, base catalogue charges, transition and exit charges - 57% Rate card - 11% Transformation & Project Delivery - 32% | Price | 35% |

## Other information

### Payment terms

Payment Structure

• Payments will be made periodically per Network Rail's Railway Period (every 4 weeks).

Invoicing and Payment Timelines

• Network Rail will pay valid, undisputed invoices within 28 days of receipt.

• Supplier must flow down prompt payment terms (28 days) to its supply chain.

Please refer to the Procurement Documents for full details.

## Description of risks to contract performance

1. Technology Risks

• Data Centre Infrastructure: Risks of physical security breaches, unauthorised access, inadequate audit controls, and failure in onsite sparing or equipment management.

• Mainframe & Platforms: Risks of service outages, backup failures, data loss, or insufficient monitoring and alerting.

• Patch Management: Risks of delayed or failed patch deployment, vulnerabilities due to unpatched systems, and errors in automated/manual patching.

• Technical Services: Risks of insufficiently certified technical resources, tooling failures, and lack of scalability or automation.

2. Network and Security Infrastructure Risks

• DC Networks: Risks of network outages, poor interconnectivity, third-party coordination failures, and WAN/LAN service disruptions.

• Perimeter Security: Risks of firewall misconfiguration, security breaches, and lack of certified network resources.

3. Application Support Risks

• Enterprise Job Scheduler: Risks of workflow automation failures, impacting business process continuity.

• Operational Support Systems: Risks of inadequate Tier 3 support, misconfiguration, or delayed updates.

• Siebel Support: Risks of application downtime, data integrity issues, and multi-server coordination failures.

4. Service Management Risks

• Availability & Capacity Management: Risks of poor performance, capacity shortfalls, and unidentified risks.

• Compliance & Information Security: Risks of non-compliance with standards, security incidents, inadequate staff vetting, and failure in digital access control.

• IT Service Continuity: Risks of ineffective disaster recovery/business continuity planning and testing.

• Service Level Management: Risks of unmet service expectations and lack of service improvement.

5. Service Transition Risks

• E-bonding & Change Management: Risks of failed data transfer, unauthorised changes, inadequate change management, and insufficiently skilled change teams.

• Knowledge & Release Management: Risks of incomplete or inaccurate knowledge transfer, poor release planning, and failed service take-on.

6. Service Operation Risks

• Event & Incident Management: Risks of poor event logging, delayed incident resolution, inadequate communication, and lack of accountability.

• Problem & Request Fulfilment: Risks of unresolved problems, poor collaboration, and delayed service requests.

• Third Party Management: Risks of SLA breaches, poor supplier coordination, and service continuity failures.

7. Continual Service Improvement Risks

• Risks of ineffective CSI initiatives, lack of monitoring, and failure to implement recommendations.

8. Governance and Reporting Risks

• Risks of inadequate governance frameworks, poor service reporting, and non-

compliance in reporting.

9. Social Value Risks

• Risks of failing to meet social value targets (jobs, skills, education), EDI requirements, SME engagement, ESG compliance, and sustainability obligations.

10. Delivery Risks

• Project Services: Risks of project delays, poor quality assurance, non-compliance with processes, and inadequate risk/issue management.

• Skilled Resources: Risks of insufficient architectural or enhancement resources, poor onboarding/offboarding, and lack of testing support.

• Third Party Management: Risks of poor operational management and reporting.

11. Transition Risks

• Risks of poor programme management, service readiness failures, inadequate knowledge transfer, asset/configuration management issues, and reduction in service performance during transition.

12. Transformation Risks

• Risks of failing to identify or deliver efficiency improvements, poor collaboration, and strategy misalignment.

13. Exit Risks

• Risks of inadequate exit planning, poor knowledge transfer, and disruption at contract end.

14. Optional Scope Risks

• Risks of poor flexibility in service take-on, inability to scale for industry transformation, and failure to support public cloud or future integration needs.

15. Legal & Compliance Risks

• Risks of non-compliance with contract management guidelines, failure to meet SLA/accountability requirements, lack of transparency in pricing, and inability to rapidly deploy certified security services.

These are risks which the Authority considers could jeopardise the satisfactory performance of the contract, but because of their nature, may not be capable of being addressed in the contract as awarded (noting that this is a competitive flexible procedure and technical dialogue and commercial negotiation are anticipated). Accordingly, these are risks that may require a subsequent modification of the contract under paragraph 5 of Schedule 8 of PA23.

## Applicable trade agreements

- Government Procurement Agreement (GPA)

- Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

## Conflicts assessment prepared/revised

Yes

# Procedure

## Procedure type

Competitive flexible procedure

## Special regime

Utilities

## Competitive flexible procedure description

Competitive Flexible Procedure

Description of stages: -

PSQ Return

Internal PSQ Evaluation

Down selection of 5 suppliers

Confidentiality Agreement execution with 5 shortlisted suppliers

ITT Publication

Clarification Sessions

ITT Responses Close

Internal ITT Evaluation

Internal ITT Moderation

ITT Supplier Presentations

Negotiation Stage 1

Negotiation Stage 2

Best and Final Offers

Award Stage

# Documents

## Documents to be provided after the tender notice

Publication of the PSQ shall be issued via Bravo. Web address is as follows: -
https://networkrail.bravosolution.co.uk/web/login.html

Documents to be published using Bravo: -

Instruction to Participants

Appendix A - Procurement Terms and Conditions

Appendix B - Conditions of Participation Criteria - PSQ

Appendix C - Tender Criteria ITT

Appendix D - Glossary

Appendix E - Overview of Requirements

Appendix Ea - Business Requirements Document

Appendix Eb - Requirements Catalogue

Appendix F - Confidentiality Agreement

Appendix G - Terms and Conditions

---

## Contracting authority

### NETWORK RAIL INFRASTRUCTURE LIMITED

• Public Procurement Organisation Number: PNZN-9524-VCQJ

Waterloo General Office

London

SE1 8SW

United Kingdom

Contact name: Sonia Diosee

Telephone: +447957726915

Email: sonia.diosee@networkrail.co.uk

Website: https://www.networkrail.co.uk/

Region: UKI45 - Lambeth

Organisation type: Public authority - central government